



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 10/736,832 Group Art Unit: 2193  
Filing Date: December 17, 2003 Examiner: Ngo, C.  
Applicant: Hee-Kwan SON  
Title: MONTGOMERY MODULAR MULTIPLIER AND METHOD  
THEREOF USING CARRY SAVE ADDITION  
Attorney Docket: 8947-000063/US

Customer Service Window  
Randolph Building  
401 Dulany Street  
Alexandria, VA 22314  
Mail Stop Amendment

February 14, 2008

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant hereby submits an Information Disclosure Statement for consideration by the Examiner.

I. LIST OF PATENTS, PUBLICATIONS, AND OTHER INFORMATION

The patents, publications and other information submitted for consideration by the Office (except unpublished U.S. patent applications) are listed on Form PTO-1449 attached hereto.

II. COPIES

A. ☒ Submitted herewith is a legible copy of (i) each foreign patent; (ii) each publication or that portion which caused it to be listed, other than U.S. patents and U.S. patent application publications unless required by the Office; (iii) for each cited pending unpublished U.S. application listed below in Section IV, the application specification including the claims, and any drawing of the application, or that portion of the application which caused it to be listed including any claims directed to that portion; and (iv) all other information or that portion which caused it to be listed.

B. ☐ Any patents, publications or other information which are listed on Form PTO-1449 or on the copies of Form PTO-892, but which are not enclosed herewith, were previously cited by or submitted to the PTO in one of the following applications which has been relied upon for an earlier filing date under 35 U.S.C. § 120:

U.S. Serial Number

U.S. Filing Date

C. ☒ Because the present application was/is being filed after June 30, 2003, no copies of the U.S. patents or U.S. patent application publications which are listed on the attached Form PTO-1449 are enclosed pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i). Any foreign patent documents or non-patent literature listed on the attached Form PTO-1449 are enclosed herewith.

D. ☐ This is a PCT application in the entry of the National Phase in the United States. A copy of the International Search Report is attached for the Examiner's information. The documents listed on the International Search Report are listed on the attached Form PTO-1449 for consideration by the Examiner and for listing on any patent resulting from this application. Since the International Search Report was from the US, EPO, or JPO search authorities, copies of these references should have been supplied to the USPTO under the trilateral agreement and are believed to be in the file of the above-identified application. (MPEP 1893.03(g))

III. CONCISE EXPLANATION OF THE RELEVANCE (check at least one box)

A. ☒ Except as may be indicated below in (B), all of the patents, publications or other information are in the English language (concise explanation not required).

B. ☒ A concise explanation of the relevance of each patent, publication or other information listed that is not in the English language is as follows (see 37 C.F.R. § 1.98(a)(3)):

1. ☒ See the attached foreign patent office communication from a counterpart foreign application:
  - European Search Report dated January 15, 2008, for European Application No. 07015586.6-2212
2. ☒ English abstracts are provided for:
  - International Patent Publication No. WO 02/073450 A1
3. ☐ Other:

C. ☒ The following additional information is provided for the Examiner's consideration.

- The following references are cited in the European Search Report dated January 15, 2008, for European Application No. 07015586.6-2212.
  1. MORITA, H., "A Fast Modular-multiplication Algorithm Based on a Radix 4 and Its Application", The Transactions of the IEICE, July 1990, pp. 1081-1086, Vol. E73, No. 7, Tokyo, JP
  2. BEHROOZ, Parhami, "High-Radix Multipliers", Computer Arithmetic: Algorithms and Hardware Design, 2000, pp. 157-171, Oxford University Press, New York, NY
  3. UK Patent Publication No. GB 2 166 894 A
- The following references are cited in the European Search Report dated January 15, 2008, for European Application No. 07015586.6-2212, but were previously cited in the Information Disclosure Statement documents filed on November 3, 2006, and May 2, 2007. Also, the Examiner has considered these references (see Examiner-initialed Form HDP-1449 in Office Action dated October 15, 2007).
  1. WANG, P. A. et al: "New VLSI Architectures of RSA Public-Key Cryptosystem" June 9, 1997, Vol. 3, pages 2040-2043
- U.S. Patent Publication No. 2004/0054705 A1 is a counterpart to International Patent Publication No. WO 02/073450 A1.

IV. CROSS REFERENCE TO RELATED APPLICATION(S)

A. ☐ The Examiner is advised that the following co-pending application(s) contain(s) subject matter that may be related to the present application. By bringing this(these) application(s) to the Examiner's attention, Applicant(s) does(do) not waive the confidentiality provisions of 35 U.S.C. § 122.

V. THIS IDS IS BEING FILED UNDER

A. ☐ 37 C.F.R. § 1.97(b): (check only one box)

1. ☐ within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d) (37 C.F.R. § 1.97(b)(1)). No fee or certification is required.

2. ☐ within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application (37 C.F.R. § 1.97(b)(2)). No fee or certification is required.

3. ☐ before the mailing of a first Office Action on the merits (37 C.F.R. § 1.97(b)(3)). No fee or certification is required. In the event that a first Office Action on the merits has been issued, please consider this IDS under 37 C.F.R. § 1.97(c) and see the certification under 37 C.F.R. § 1.97(e) below; or, if no certification has been made, charge our deposit account a fee in the amount of \$180.00 as required by 37 C.F.R. § 1.17(p).

4. ☐ before the mailing of a first Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114. No fee or certification is required.

B. ☒ 37 C.F.R. § 1.97(c): (check only one box)

☒ before the mailing date of either any Final Office Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an action that otherwise closes prosecution.

1. ☐ No certification; therefore, a fee in the amount of \$180.00 is required by 37 C.F.R. § 1.17(p).

2. ☒ See the certification below. No fee is required.

C. ☐ 37 C.F.R. § 1.97(d):

☐ after the mailing date of either a Final Office Action under 37 C.F.R. § 1.113 or a Notice of Allowance under 37 C.F.R. § 1.311, yet on or before payment of the issue fee.

1. ☐ See the certification below. A fee in the amount of \$180.00 is required by 37 C.F.R. § 1.17(p).

VI. CERTIFICATION UNDER 37 C.F.R. § 1.97(e): (check only one box)

The undersigned hereby certifies that:

- A. ☒ each item of information contained in this IDS was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS (See 37 C.F.R. § 1.97(e)(1)). See further statement under 37 C.F.R. § 1.704(d) below in section VII, if applicable; or
- B. ☐ no item of information contained in this IDS was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this IDS was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this IDS (See 37 C.F.R. § 1.97(e)(2)).
- C. ☐ Some of the items of information were first cited in a communication from a foreign patent office. As to this information, the undersigned hereby certifies that each item of information contained in this IDS was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS. As to the remaining information, the undersigned hereby certifies that no item of this remaining information contained in this IDS was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this IDS was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this IDS.

VII. STATEMENT UNDER 37 C.F.R. § 1.704(d)

The undersigned hereby states that:

☐ each item of information contained in this IDS was cited in a communication from a foreign patent office in a counterpart application and this communication was not received by any individual designated in 37 C.F.R. § 1.56(c) more than thirty days prior to the filing of this IDS.

VIII. PAYMENT OF FEES (check only one box)

- A. ☒ No fee is believed to be due in light of the above-noted status or above-provided certification.
- B. ☐ A check in the amount of \$180.00 is enclosed for the above-identified fee.
- C. ☐ Please charge Deposit Account No. 08-0750 in the amount of \$180.00 for the above-indicated fee. A duplicate copy of this paper is attached.

The above references are being cited only in the interest of candor and without any admission that they constitute statutory prior art, contain matter which anticipates the invention, or which would render the same obvious, either singly or in combination, to a person of ordinary skill in the art. Furthermore, this Information Disclosure Statement shall not be construed as a representation that a search has been made.

If it is determined that this IDS has been filed under the wrong rule, the PTO is requested to consider this IDS under the proper rule (with a petition if necessary) and charge the appropriate fee to Deposit Account No. 08-0750.

Please charge any additional fees or credit any overpayment pursuant to 37 C.F.R. §§ 1.16 or 1.17 to Deposit Account No. 08-0750.

Respectfully submitted,

HARNESS, DICKEN, & PIERCE, P.L.C.

By: \_\_\_\_\_

John A. Castellano, Reg. No. 35,094

P.O. Box 8910  
Reston, Virginia 20195  
(703) 668-8000

JAC/LFG/cm

Enclosures:



Form HDP-1449, listing 7 references and submitting 5 references (1 p.)

References:

1. European Search Report dated January 15, 2008, for European Application No. 07015586.6-2212 (17 pp.)
2. International Patent Publication No. WO 02/073450 A1(78 pp.)
3. MORITA, H., "A Fast Modular-multiplication Algorithm Based on a Radix 4 and Its Application", The Transactions of the IEICE, July 1990, pp. 1081-1086, Vol. E73, No. 7, Tokyo, JP (6 pp.)
4. BEHROOZ, Parhami, "High-Radix Multipliers", Computer Arithmetic: Algorithms and Hardware Design, 2000, pp. 157-171, Oxford University Press, New York, NY (15 pp.)
5. UK Patent Publication No. GB 2 166 894 A (20 pp.)